may deliver its privacy notice according to § 40.6(d)(3).

§ 40.5 Annual privacy notice to customers required.

(a)(1) *General rule.* A bank must provide a clear and conspicuous notice to customers that accurately reflects its privacy policies and practices not less than annually during the continuation of the customer relationship. *Annually* means at least once in any period of 12 consecutive months during which that relationship exists. A bank may define the 12-consecutive-month period, but the bank must apply it to the customer on a consistent basis.

(2) *Example.* A bank provides a notice annually if it defines the 12-consecutive-month period as a calendar year and provides the annual notice to the customer once in each calendar year following the calendar year in which the bank provided the initial notice. For example, if a customer opens an account on any day of year 1, the bank must provide an annual notice to that customer by December 31 of year 2.

(b)(1) *Termination of customer relationship.* A bank is not required to provide an annual notice to a former customer.

(2) *Examples.* A bank's customer becomes a former customer when:

(i) In the case of a deposit account, the account is inactive under the bank's policies;

(ii) In the case of a closed-end loan, the customer pays the loan in full, the bank charges off the loan, or the bank sells the loan without retaining servicing rights;

(iii) In the case of a credit card relationship or other open-end credit relationship, the bank no longer provides any statements or notices to the customer concerning that relationship or the bank sells the credit card receivables without retaining servicing rights; or

(iv) The bank has not communicated with the customer about the relationship for a period of 12 consecutive months, other than to provide annual privacy notices or promotional material.

(c) *Special rule for loans.* If a bank does not have a customer relationship with a consumer under the special rule for loans in § 40.4(c)(2), then the bank need not provide an annual notice to that consumer under this section.

(d) *Delivery.* When a bank is required to deliver an annual privacy notice by this section, the bank must deliver it according to § 40.9.

§ 40.6 Information to be included in privacy notices.

(a) *General rule.* The initial, annual, and revised privacy notices that a bank provides under §§ 40.4, 40.5, and 40.8 must include each of the following items of information, in addition to any other information the bank wishes to provide, that applies to the bank and to the consumers to whom the bank sends its privacy notice:

(1) The categories of nonpublic personal information that the bank collects;

(2) The categories of nonpublic personal information that the bank discloses;

(3) The categories of affiliates and nonaffiliated third parties to whom the bank discloses nonpublic personal information, other than those parties to whom the bank discloses information under §§ 40.14 and 40.15;

(4) The categories of nonpublic personal information about the bank's former customers that the bank discloses and the categories of affiliates and nonaffiliated third parties to whom the bank discloses nonpublic personal information about the bank's former customers, other than those parties to whom the bank discloses information under §§ 40.14 and 40.15;

(5) If a bank discloses nonpublic personal information to a nonaffiliated third party under § 40.13 (and no other exception in §§ 40.14 or 40.15 applies to that disclosure), a separate statement of the categories of information the bank discloses and the categories of third parties with whom the bank has contracted;

(6) An explanation of the consumer's right under § 40.10(a) to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right at that time;

(7) Any disclosures that the bank makes under section 603(d)(2)(A)(iii) of the Fair Credit Reporting Act (15

U.S.C. 1681a(d)(2)(A)(iii)) (that is, notices regarding the ability to opt out of disclosures of information among affiliates);

(8) The bank's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; and

(9) Any disclosure that the bank makes under paragraph (b) of this section.

(b) *Description of nonaffiliated third parties subject to exceptions.* If a bank discloses nonpublic personal information to third parties as authorized under §§ 40.14 and 40.15, the bank is not required to list those exceptions in the initial or annual privacy notices required by §§ 40.4 and 40.5. When describing the categories with respect to those parties, the bank is required to state only that it makes disclosures to other nonaffiliated third parties as permitted by law.

(c) *Examples*—(1) *Categories of nonpublic personal information that the bank collects.* A bank satisfies the requirement to categorize the nonpublic personal information that it collects if it lists the following categories, as applicable:

(i) Information from the consumer;

(ii) Information about the consumer's transactions with the bank or its affiliates;

(iii) Information about the consumer's transactions with nonaffiliated third parties; and

(iv) Information from a consumer reporting agency.

(2) *Categories of nonpublic personal information the bank discloses.* (i) A bank satisfies the requirement to categorize the nonpublic personal information that it discloses if the bank lists the categories described in paragraph (e)(1) of this section, as applicable, and a few examples to illustrate the types of information in each category.

(ii) If a bank reserves the right to disclose all of the nonpublic personal information about consumers that it collects, it may simply state that fact without describing the categories or examples of the nonpublic personal information it discloses.

(3) *Categories of affiliates and nonaffiliated third parties to whom the bank discloses.* A bank satisfies the requirement to categorize the affiliates and nonaffiliated third parties to whom it discloses nonpublic personal information if the bank lists the following categories, as applicable, and a few examples to illustrate the types of third parties in each category:

(i) Financial service providers;

(ii) Non-financial companies; and

(iii) Others.

(4) *Disclosures under exception for service providers and joint marketers.* If a bank discloses nonpublic personal information under the exception in § 40.13 to a nonaffiliated third party to market products or services that it offers alone or jointly with another financial institution, the bank satisfies the disclosure requirement of paragraph (a)(5) of this section if it:

(i) Lists the categories of nonpublic personal information it discloses, using the same categories and examples the bank used to meet the requirements of paragraph (a)(2) of this section, as applicable; and

(ii) States whether the third party is:

(A) A service provider that performs marketing services on the bank's behalf or on behalf of the bank and another financial institution; or

(B) A financial institution with whom the bank has a joint marketing agreement.

(5) *Simplified notices.* If a bank does not disclose, and does not wish to reserve the right to disclose, nonpublic personal information about customers or former customers to affiliates or nonaffiliated third parties except as authorized under §§ 40.14 and 40.15, the bank may simply state that fact, in addition to the information it must provide under paragraphs (a)(1), (a)(8), (a)(9), and (b) of this section.

(6) *Confidentiality and security.* A bank describes its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information if it does both of the following:

(i) Describes in general terms who is authorized to have access to the information; and

(ii) States whether the bank has security practices and procedures in place to ensure the confidentiality of the information in accordance with the bank's policy. The bank is not required

to describe technical information about the safeguards it uses.

(d) *Short-form initial notice with opt out notice for non-customers.* (1) A bank may satisfy the initial notice requirements in §§ 40.4(a)(2), 40.7(b), and 40.7(c) for a consumer who is not a customer by providing a short-form initial notice at the same time as the bank delivers an opt out notice as required in § 40.7.

(2) A short-form initial notice must:

(i) Be clear and conspicuous;

(ii) State that the bank's privacy notice is available upon request; and

(iii) Explain a reasonable means by which the consumer may obtain that notice.

(3) The bank must deliver its short-form initial notice according to § 40.9. The bank is not required to deliver its privacy notice with its short-form initial notice. The bank instead may simply provide the consumer a reasonable means to obtain its privacy notice. If a consumer who receives the bank's short-form notice requests the bank's privacy notice, the bank must deliver its privacy notice according to § 40.9.

(4) *Examples of obtaining privacy notice.* The bank provides a reasonable means by which a consumer may obtain a copy of its privacy notice if the bank:

(i) Provides a toll-free telephone number that the consumer may call to request the notice; or

(ii) For a consumer who conducts business in person at the bank's office, maintain copies of the notice on hand that the bank provides to the consumer immediately upon request.

(e) *Future disclosures.* The bank's notice may include:

(1) Categories of nonpublic personal information that the bank reserves the right to disclose in the future, but do not currently disclose; and

(2) Categories of affiliates or nonaffiliated third parties to whom the bank reserves the right in the future to disclose, but to whom the bank does not currently disclose, nonpublic personal information.

(f) *Sample clauses.* Sample clauses illustrating some of the notice content required by this section are included in Appendix A of this part.

§ 40.7 Form of opt out notice to consumers; opt out methods.

(a) (1) *Form of opt out notice.* If a bank is required to provide an opt out notice under § 40.10(a), it must provide a clear and conspicuous notice to each of its consumers that accurately explains the right to opt out under that section. The notice must state:

(i) That the bank discloses or reserves the right to disclose nonpublic personal information about its consumer to a nonaffiliated third party;

(ii) That the consumer has the right to opt out of that disclosure; and

(iii) A reasonable means by which the consumer may exercise the opt out right.

(2) *Examples.* (i) *Adequate opt out notice.* A bank provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if the bank:

(A) Identifies all of the categories of nonpublic personal information that it discloses or reserves the right to disclose, and all of the categories of nonaffiliated third parties to which the bank discloses the information, as described in § 40.6(a)(2) and (3), and states that the consumer can opt out of the disclosure of that information; and

(B) Identifies the financial products or services that the consumer obtains from the bank, either singly or jointly, to which the opt out direction would apply.

(ii) *Reasonable opt out means.* A bank provides a reasonable means to exercise an opt out right if it:

(A) Designates check-off boxes in a prominent position on the relevant forms with the opt out notice;

(B) Includes a reply form together with the opt out notice;

(C) Provides an electronic means to opt out, such as a form that can be sent via electronic mail or a process at the bank's web site, if the consumer agrees to the electronic delivery of information; or

(D) Provides a toll-free telephone number that consumers may call to opt out.

(iii) *Unreasonable opt out means.* A bank *does not* provide a reasonable means of opting out if: